European Economic Interest Group-
European Rail Traffic Management System.
133 Rue Froissart - 1040 Brussels - Belgium.
Phone (02) 673-99-33/fax 673-41-50. TVA 455-935.830

Reference EEIG : 04E083

Distribution date : 12.12.05
Document version : 1.0

Safety Requirements and

Requirements to Safety Analysis for Interoperability

for the

Control-Command and Signalling Sub-System.

Version and Modifications

Version No.	Date of distribution	Comments on the modification	Responsible for the modification
1.0 D1	3 Mar 2005	First draft derived from Justification Report 1.0 D10	KA and RD
1.0 D1.1	24 Mar 2005	Comments from ISA and working group included	Working group
1.0 D1.2	8 April 2005	General update and title changed	Working group
1.0 D1.3	29 June 2005	Comments from the ISA group implemented	KA, FL and LN
1.0 D1.4	15 July 2005	Comments from the ISA group implemented after meeting 6 July	KA, FL and LN
1.0 D1.5	28 July 2005	References in document updated	KA
1.0	12-12-05	Version for formal distribution	RD

CONTENTS

1 Introduction

1.1 General

1.1.1.1 This document “Safety Requirements and Requirements to Safety Analysis for Interoperability for the Control-Command and Signalling Sub-System” (Index 47) has been produced as a normative document to provide the Safety Requirements necessary for the Control-Command and Signalling Technical Specification for Interoperability for both High Speed {Ref.: 4} and Conventional Rail CCS CR TSI {Ref.: 5}.

In the following “CCS TSI” is used and covers both TSIs.

1.1.1.2 This document is supported by a Justification Report {Ref.: 1}, which may be consulted for further explanations, justifications and derivations. The Justification Report comprises a list of open points and recommends essential future actions to be carried out. The future actions are amongst other things designated to achieve harmonised THRs and to apportion them to on-board and track-side.

1.1.1.3 In the current version of the document the THRs have not been harmonised, therefore chapter 6 includes examples of THRs from different countries. Throughout the document the text has been written as if harmonised THRs had been achieved.

1.1.1.4 Chapter 2 clarifies the scope of this document and

Chapter 3 provides a summary of the Rationale behind the approach.

Chapter 4 clarifies the definition of the Control-Command and Signalling system for the purpose of safety requirements by presenting a System Definition.

Chapter 5 lists the System Hazards.

Chapter 6 presents the quantitative safety requirements

1.2 Status of Document

1.2.1.1 The whole document - except for chapter 6.2 and 6.3 - is mandatory as long as the THRs are not harmonised, in order to achieve harmonisation. Chapter 6.2 and 6.3 is not mandatory as long as it contains only national examples. After harmonisation of the Safety Requirements, the national examples will be replaced by the harmonised THRs. Then the mandatory part of the document will then be chapter 5 and 6 only.

2 Scope

2.1.1.1 This document specifies the Safety Requirements for the Conventional Rail and High Speed Control-Command and Signalling sub-system as defined in Directives 96/48/EC {Ref.: 2} and 01/16/EC {Ref.: 3}. All safety requirements necessary for interoperability from a Control-Command and Signalling perspective are included. According to EN 50129 additional analyses is necessary based on the system design (Causes for Hazards, Apportionment of safety targets).

2.1.1.2 The apportionment of safety targets, concerning ETCS, is done in Index 27 / Subset 91 {Ref.: 6} for the 'ETCS core hazard' (Exceeding of the safe speed / distance as advised to ETCS).

2.1.1.3 The scope of the Safety Requirements in the Index 47 Document is to cover part of phase 3 (EN 50126). It is not the intention to cover the whole Life Cycle of CCS TSI.

2.1.1.4 ERTMS Level 3 has been excluded from the scope of Index 47.

2.1.1.5 The scope has been aligned to the TSI CCS scope. This was decided through the political processes including Article 21 Committee. The TSI scope can not in itself guarantee safety of the system since the National part and an interface to it is outside the TSI scope.

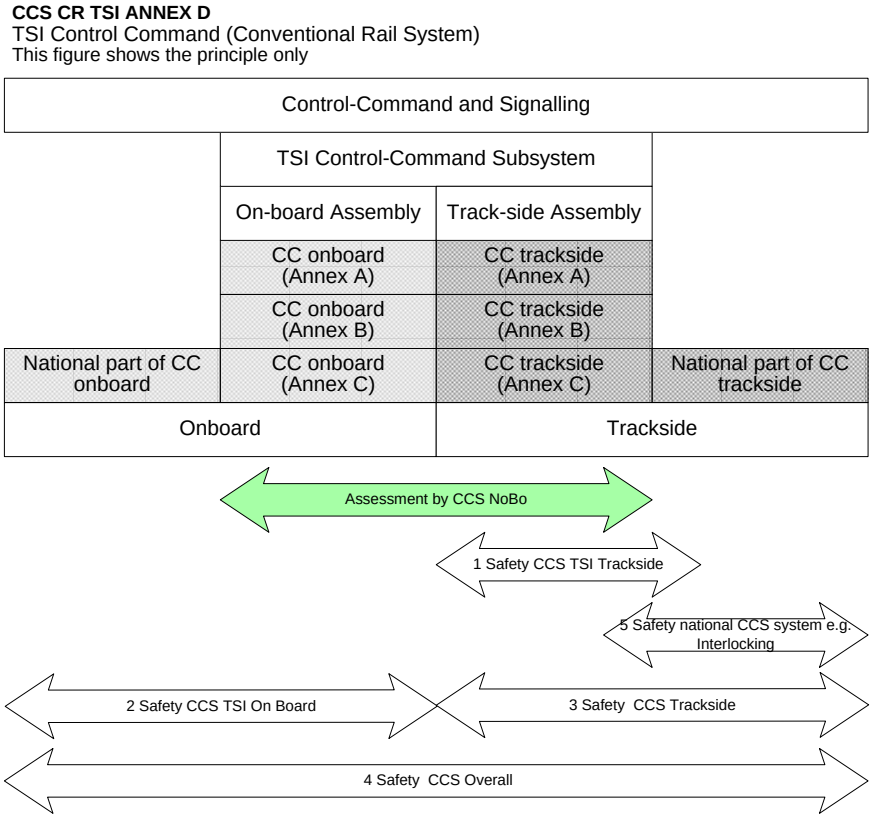


Figure 1 – Scope Diagram

3 Rationale

3.1 General

3.1.1.1 The Rationale behind this document is the need of harmonising safety requirements applicable to Control-Command and Signalling sub-system, to the extent that they affect interoperability.

3.1.1.2 This will allow

a) the comparison of the different national safety targets

b) the harmonisation of the mandatory safety requirements

and in future

c) safety requirements to be apportioned (and harmonised) between on board (OBU) and track-side (RBCs, balises) and if necessary to single constituents.

3.1.1.3 This plays an important role to allow

- Certification of Control-Command and Signalling interoperability constituents
- Verification of Control Command and Signalling track-side and on-board assemblies

3.1.1.4 In a way that permits the authorisation to service, respecting the required safety objectives and allowing

- interoperable trains to be accepted without the need for additional verification of Control-Command and Signalling aspects and
- those aspects of infrastructure concerned with interoperability not to require additional verification in terms of running an interoperable train.

3.1.1.5 Acceptance of the overall trackside arrangements in a way that satisfies the safety objectives for the train service is a National issue.

3.1.1.6 The process used in the development of the safety requirements consists of 6 steps:

Step 1: Detailed System Definition – System Structure
Step 2: Detailed System Definition – Functional Analysis
Step 3: Hazard Identification
Step 4: Identification of System Hazards
Step 5: Systematic check of the inputs and outputs to the CCS TSI system for consistency reasons
Step 6: Introduction of safety requirements to CCS TSI System Hazards

3.2 Completeness of hazard identification

3.2.1.1 In order to ensure completeness of the system hazards identified, different approaches and methods are merged. The resulting synergetic effect ensures completeness at Risk Analysis level without the consideration of the technical solution (e.g. detailed ETCS specific functions).

Methods:

3.2.1.2 Functional approach to hazard identification on operational level

3.2.1.3 Analysis of a generic train mission including consideration of preparatory conditions

3.2.1.4 Verification of functional approach by ensuring coverage of functions listed in 'Analysis of Trans-European Rail Operation' {Ref.: 8}

3.2.1.5 Causal Analysis drawing links within the defined system and analysing all causes for system hazards

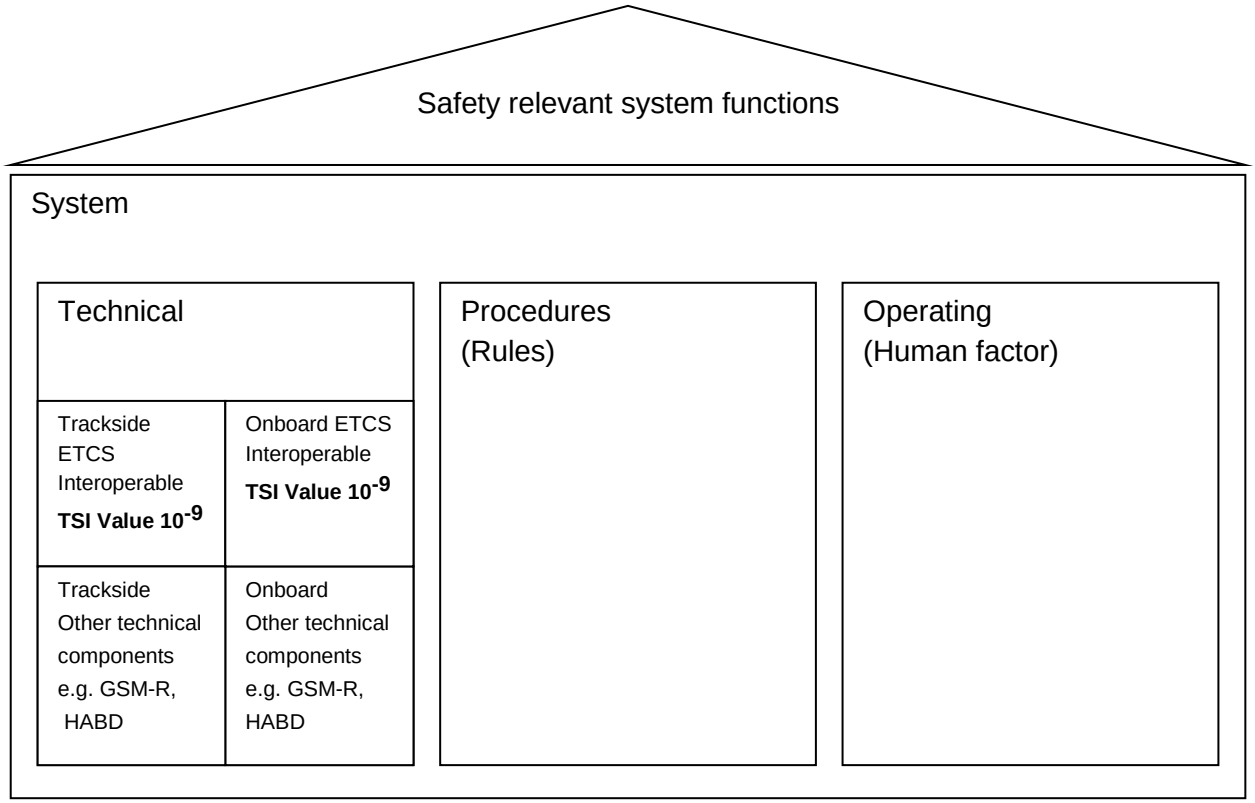
4 System Definition

4.1 General

4.1.1.1 The system definition is based on the CCS TSI.

4.1.1.2 To ensure safety the technical and operational aspects must be analysed together and this has been done to derive the safety requirements stated in this document.

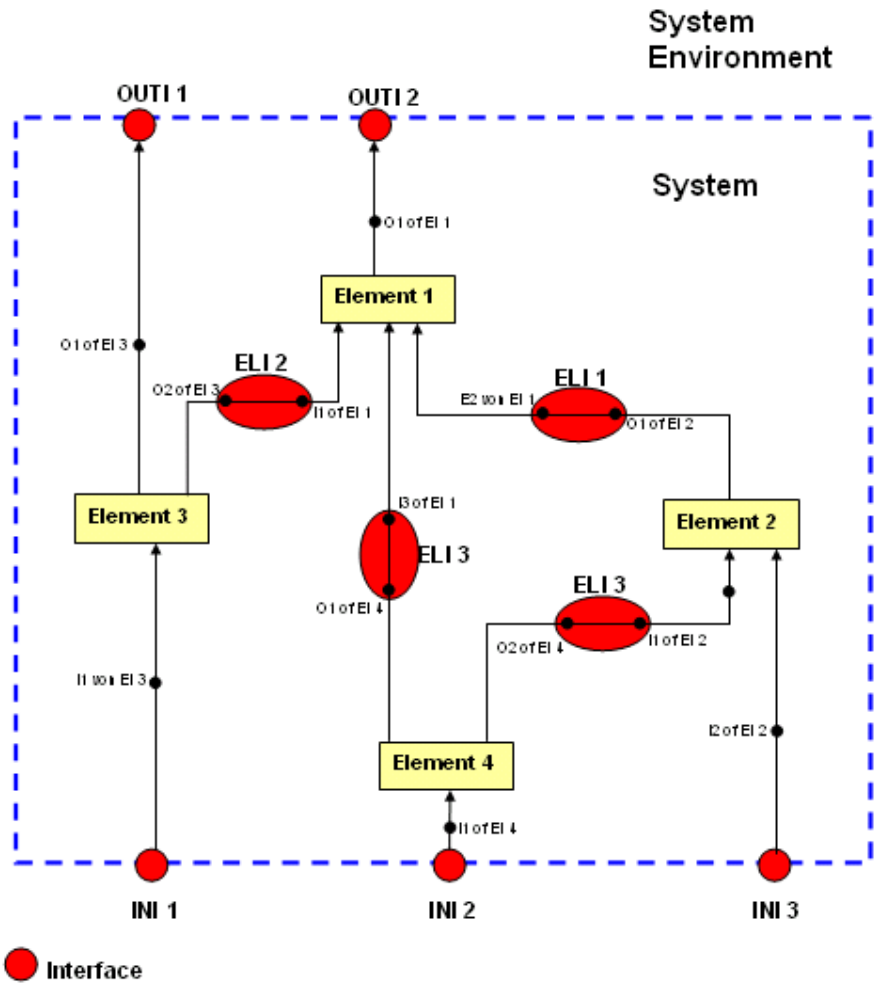
4.1.1.3



4.1.1.4 The purpose of this analysis is to provide a definition of the system structure of the Control Command and Signalling TSI subsystem in the context of safety analysis. The task is to firstly derive an architectural structure according to the 'Model of system structure' including elements, interfaces and boundaries and secondly a functional system definition.

4.2 Model of system structure

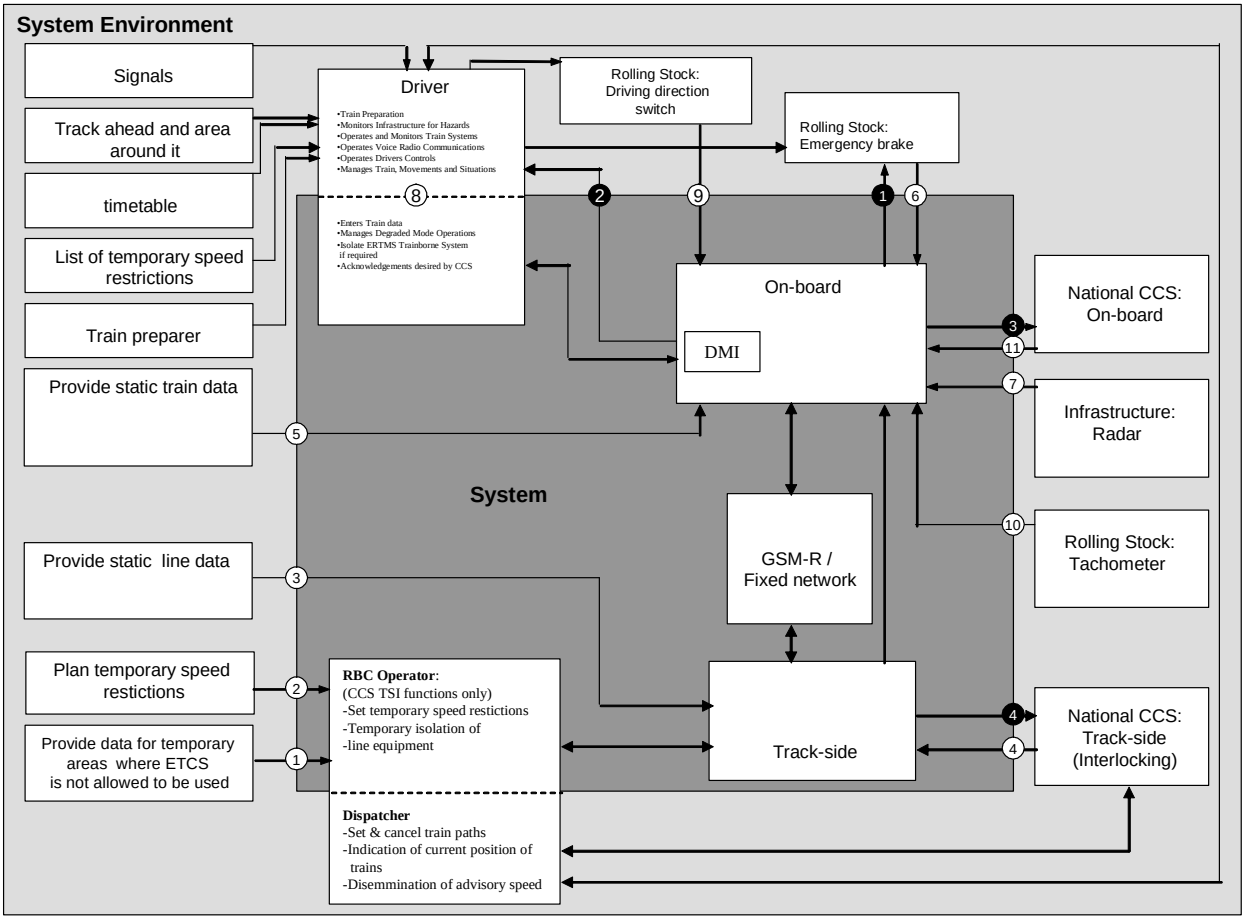
4.2.1.1 As basis for the derivation of the system architecture a general 'Model of system structure' was applied.



OUTI	Output interface (system >>> system environment)
INI	Input interface (system environment >>> system)
ELI	Element interface (element >>> element)
Ix	Input no. x
Ox	Output no. x
Elx	Element no. x

4.3 System architecture

4.3.1.1 The following drawing was developed on basis of the 'Model of System Structure'. It describes the architecture of the System including interfaces, elements and boundaries. This System Architecture drawing is used for the process of hazard identification.



x Output Interface No. X

Y Input Interface No. Y

4.3.1.2 Note 1

The System as described in 4.3.1.1 is dependant on other systems: Other systems may influence the defined system via the input interfaces. In the context of Index 47, other systems influencing the defined system are considered as being ideal (functioning without errors). Nevertheless, if the scope of safety assessment is expanded to the overall safety of railways, the influence of the other systems have to be considered.

4.3.1.3 Note 2

The analysis and evaluation of the link between input and output interfaces within the defined System (4.3.1.1) is the task of the Causal Analysis, according to the applied safety concept (see Justification Report {Ref.:1. §2.2}).

4.3.1.4 Note 3

The driver and RBC operator/dispatcher are partly within and partly outside the system borders according to the functionality fulfilled. The driver is usually one person, whereas the RBC operator/dispatcher may be two different persons

4.4 Output Interfaces

4.4.1.1 This table lists the output interfaces of the System architecture and exemplarily describes the information transmitted. Unlike the input interfaces, the output interfaces play a major role during the process of hazard identification. The input interfaces will be considered in the Causal Analysis.

Interface #	Interface between	Direction	and:	Description	UNISIG reference {Ref.: 7}
1	CCS TSI: On-Board	→	Rolling Stock: Emergency brake	- braking command	SUBSET 031 (2.0.0), page 8, figure 1: *'train order'*
2	CCS TSI: On-Board	→	OPE: Driver	e.g.: - 'ETCS ready-to-operate' indication - ETCS mode indication - ETCS level indication - actual speed indication - supervised maximum speed indication - distance to brake target indication - predicted speed at brake target indication - Auxiliary Driving Information (e.g. approaching a tunnel or lowering the pantograph) - text messages - acknowledgement request - emergency stop (via GSM-R voice)	SUBSET 031 (2.0.0), page 8, figure 1: *'MMI indication'*
3	CCS TSI: On-board	→	National CCS: On-board	- activation command for national CCS	SUBSET 091 (2.2.2), chapter 2, 2.5.3: *'STM'*
4	CCS TSI: Track-side	→	National CCS: Trackside	- synchronisation request - emergency stop notification	SUBSET 032 (2.0.0), page 7, figure 1: *'RBC information'*

4.5 Detailed System Definition - Functional Analysis

4.5.1.1 In order to apply a functional approach to hazard identification the following table was developed basing on the 'Functional Analysis of Trans-European rail operation' {Ref.: 8}. This reveals a functional system definition and it consists of functions relevant for CCS TSI exclusively.

4.5.1.2 Functions considered in the functional approach, but not relevant for CCS TSI, are listed in the Justification report {Ref.: 1}

Ref.	Functions relevant for railway operation		Function relevant for CCS TSI	
	Function	Annotations	X	Explanation
2	**Prepare move**			
2.3	Forming the train			
2.3.5	documenting formation of train		**X**	information about braking characteristics
2.4	Checking that train is safe to operate and fit to run	Not a basic function of running; has purpose of establishing »safe condition of vehicles«.		
2.4.3	establish condition and fitness for function of vehicle's brakes		**X**	functionality of brakes is prerequisite for correct calculation of braking curves
2.4.4	»train initialisation«	Train number, max. permissible speed, effective braking power, length, load if applicable.	**X**	information necessary
2.5.4	special features of movement		**X**	relevant for route suitability
4	**Set up conditions for move**			
4.7	Maintaining headways	Exclusion of moves that might endanger each other		
4.7.2	protection against opposing moves	Opposing moves also include movements in the opposite direction to that allowed (e.g. inadmissible setting back).	**X**	function partly executed in the interlocking
4.8	Protection against unintended movements by vehicles			
4.8.2	shunting prohibited		**X**	
5	**Authorising move**			
5.1	Convey orders/authorisations	No case for further subdivisions at this point, since it is already necessary to cite solutions (e.g. optical, written, acoustical orders, ...)	**X**	
6	**Perform move**			

6.1	Observing/obeying to max. permissible speeds			
6.1.1	taking account of line-related restrictions			
6.1.1.1	max. permissible speed as a function of track layout	Restriction due to radius of curves, cant, transition curves and length of cant gradient	**X**	
6.1.1.2	max. permissible speed when passing switches	Restrictions in the deflecting or more tightly curved section of the switch and in the case of trailable points.	**X**	
6.1.1.3	max. permissible speed when passing level crossings	Restriction of top speed, speed as a function of the length of the strike-in section.	**X**	
6.1.1.4	max. permissible speed on bridges		**X**	
6.1.1.5	max. permissible speed on embankments		**X**	
6.1.1.6	max. permissible speed due to the superstructure		**X**	
6.1.1.7	max. permissible speed due to the subgrade		**X**	
6.1.1.8	max. permissible speed due to the catenary design		**X**	
6.1.1.9	max. permissible speed at sections tight on gauge	if distance between tracks insufficient in terms of the kinematic envelope.	**X**	covered by function 6.2.10
6.1.1.10	max. permissible speed in the event of deviations in track elements from nominal state (with reference to movement at a defined speed)	Switch without signal interlocking, technical protection at level crossing has failed.	**X**	
6.1.1.11	max. permissible speed following engineering work		**X**	
6.1.2.1	max. permissible speed of train due to running properties of vehicles		**X**	
6.1.2.2	max. permissible speed due to braking properties of vehicles		**X**	
6.1.2.3	max. permissible speed in event of deviations from nominal state of vehicle components with a bearing on safety (with reference to movement at a defined speed)		**X**	
6.1.2.4	max. permissible speed when movements meet		**X**	
6.1.2.5	max. permissible speed in the event of cross-winds		**X**	
6.1.3	taking account of procedure-related restrictions			
6.1.3.1	max. permissible speed when running on sight	Observing this speed is not a function required in itself to guarantee safety; the intention, instead, is to facilitate performance of the »Stop at required point« function.	**X**	
6.1.3.2	max. permissible shunting speed	as above	**X**	
6.1.3.3	max. permissible speed for banked movements	as above		
6.1.3.4	max. permissible speed when setting back in the event of danger	as above	**X**	
6.1.3.5	max. permissible speed when entering dead-end tracks	as above	**X**	
6.1.3.6	max. permissible speed when entering partially occupied tracks	as above	**X**	
6.1.3.7	max. permissible speed for reasons of safety of track works	not a function for protecting movement	**X**	
6.1.3.8	max. permissible speed in case of temporary speed restrictions		**X**	

6.2	Observing (further) line-related restrictions			
6.2.1	lower pantograph(s) at required point	Turntables, traversers, crane trackage, other sections without catenary or to be passed with pantograph down.	**X**	
6.2.2	switch off motive power unit current (main switch off) at required point	Insulated sections, changes of system, depot gates with insulated catenary adaptor.	**X**	
6.2.8	avoid stopping at points not suitable for the adoption of auxiliary measures or only poorly so	Emergency brake override; function is only of relevance, however, in the event of an incident (notably fire).	**X**	
6.2.9	take account of restrictions in the use of specified brake designs	e.g. eddy-current brake	**X**	
6.2.10	Prove reliability of movement	- loading gauge - power supply - axle load	**X**	route suitability
6.2.11	Reversing in the event of danger	ERTMS/ETCS FRS 11.3.2 and SRS 4.4.18 and 5.13	**X**	
6.4	Ensure stops required for reasons of safety			
6.4.1	stopping at a signal at danger	Cab display is synchronised with signals at danger. This includes the provision that onward movement following a stopping event may only occur once the stop has been revoked.	**X**	
6.4.2	stopping before stationary vehicles	to the extent that vehicles are not protected by signals at danger (depending on the mode of operation)	**X**	
6.4.3	stopping at track closings	Reference may not be necessary, since track closings are indicated by means of signals at danger.	**X**	
6.4.4	stopping before other obstacles (than vehicles) on the track	to the extent that the movement has been specifically authorised to do so.	**X**	
6.6	Check for safety-related deviations to railway installations on used route and adopt measures	Not a basic function of train running; serves to ensure the »safe state of railway installations«.	**X**	
6.7	Check for safety-related deviations to vehicles on the movement concerned and adopt measures	Not a basic function of train running; serves to ensure the »safe state of railway installations«.		
6.7.3	irregularities in the vehicle's safety equipment		**X**	
7	**Conclude move**			
7.2	Protecting parked vehicles			
7.2.1	applying brakes		**X**	
8	**Miscellaneous**			
8.2.3	accident investigation		**X**	juridical recording
8.3	Ensure safe condition of railway infrastructure		**X**	
8.4	Ensure safe condition of vehicles		**X**	
8.5	Formation, Training and Qualification	comprises safety instructions, accident prevention und 'safety at work'	**X**	

5 Hazard Identification

5.1 General

5.1.1.1 This chapter presents the result of the hazard identification: the list of System hazards.

5.1.1.2 The hazard identification is based on the abstract and functional system definition (chapter 4). For this reason the hazards identified are independent of specific realisations or applications. Specific realisations or circumstances are to be taken into consideration by the Causal Analysis, which evaluates/analyses the technical solution in order to identify causes for hazards and verify if new hazards arise from system design.

5.1.1.3 Common Cause.

Two ore more hazards may occur together as a result of a common cause. The consideration and evaluation of common causes is the task of a Causal Analysis, as defined in EN 50129 (Figure A.2).

5.1.1.4 Link of Causes to System Hazards.

According to EN50129 figure A.4 shows, that the cause of a hazard at system level (Hazard Type A) may be considered as a hazard at subsystem level (Hazard Type B). A link of Hazards Type B towards hazard(s) Type A can be drawn by a structured hierarchical approach to hazard analysis and hazard tracking. Table E.6 of EN50129 provides methods for failure and hazard analysis. According to A.4.2 of EN 50129, the supplier carries out a Causal Analysis, which includes the analysis of system/sub-system to meet the requirements. Concluding, EN 50129 reveals, that the link of Hazards Type B towards Hazards Type A is analysed while carrying out a Causal Analysis

5.1.1.5 A hazard is considered to be a System hazard if the failure mode of a function, relevant for CCS TSI, could lead to an accident and is allocated at an output interface of the defined system.

5.1.1.6 For Step 3 'Hazard Identification' (3.1.1.6) the following detailed process is applied.

5.1.1.7 Step 3.1: Application of failure modes to the relevant functions:

Failure modes of CCS TSI relevant functions are CCS TSI relevant hazards.

5.1.1.8 Step 3.2: Check for safety relevance:

CCS TSI relevant hazards are to be checked, if they are safety relevant or not, based on a simplified consequence analysis. If there is a probability higher than 0 of an accident as a consequence of a CCS TSI relevant hazard, the hazard is safety relevant.

Only CCS TSI relevant hazards which are safety relevant are kept for further consideration.

5.1.1.9 Step 3.3: System border check:

As final step the resulting hazards from step 3.2 are put to a 'system border check' to decide about the allocation of the hazard in the System Architecture (4.3.1.1). If a hazard is located at an output interface, it is a System hazard to be put into the Log of System Hazards.

5.2 Log of System hazards

5.2.1.1 The following table states the System Hazards resulting from the hazard identification.

5.2.1.2 The hazards exclusively apply to that part of functionality which is fulfilled by the defined system.

No.	Ref.	System hazard	Allocation to Output Interface No. (see 4.4.1.1)
1	[4.7.2-2]	unauthorised setting back	1
2	[4.8.2]	passing the defined border of the shunting area (balise 'stop if in shunting')	1
3	[5.1-2]	move inadmissibly authorised	2
4	[5.1-3]	permission to proceed not withdrawn in time in the event of danger	2
5	[6.1-0]	permissible speed as a function of route characteristics incorrectly shown	2
6	[6.1-1]	permissible speed as a function of route characteristics not enforced	1
7	[6.1.1.3-0]	permissible speed when passing level crossings incorrectly shown	2
8	[6.1.1.3-1]	permissible speed when passing level crossings not enforced	1
9	[6.1.1.8-0]	permissible speed on account of the design of the overhead line incorrectly shown	2
10	[6.1.1.8-1]	permissible speed on account of the design of the overhead line not enforced	1
11	[6.1.2.1-0]	permissible speed of train due to running properties of vehicles incorrectly shown	2
12	[6.1.2.1-1]	permissible speed of train due to running properties of vehicles not enforced	1
13	[6.1.3.1-0]	permissible speed when running on sight incorrectly shown	2
14	[6.1.3.1-1]	permissible speed when running on sight not enforced	1

15	[6.1.3.2-0]	permissible shunting speed incorrectly shown	2
16	[6.1.3.2-1]	permissible shunting speed not enforced	1
17	[6.1.3.4-0]	permissible speed when reversing in the event of danger incorrectly shown	2
18	[6.1.3.4-1]	permissible speed when reversing in the event of danger not enforced	1
19	[6.1.3.7-0]	permissible speed on grounds of track works incorrectly shown	2
20	[6.1.3.7-1]	permissible speed on grounds of track works not enforced	1
21	[6.2.1-0]	lowering pantograph indication incorrectly shown	2
22	[6.2.8]	stopping at points where stopping is not permitted	2
23	[6.2.10-0]	Information about route unsuitability not advised to the driver	2
24	[6.2.10-1]	enter a section of the route which is not permitted to (due to route suitability)	1
25	[6.2.11]	Authorisation for reversing in the event of danger not given	
26	[6.4.1-1]	not stopping at the end of a movement authoritiy (without stopping beyond the end of movement authority)	1
27	[6.4.1-2]	not stopping at the end of a movement authoritiy (but stopping beyond the end of movement authority)	1
28	[6.4.1-3]	start moving without having a correct movement authority	1
29	[7.2.1]	air brake not applied when vehicle parked	1

6 Control-Command and Signalling Safety Requirements

6.1 General

This chapter contains so far examples of national safety requirements and is therefore a non-mandatory part of this document. Some work is still to be done in order to enable harmonisation of THRs and SILs imposed on the System Hazards, constituting the harmonised safety requirements for CCS for interoperability: First the comparison of national examples for safety requirements has to be triggered. Therefore the member states are asked to contribute to chapter 6 of the document - following the process prescribed in Index 47 - deriving national values for THRs (In order to achieve a high level of comparability, assumptions about Level of tolerable Risk, Criticality, Fatality and the apportionment of the tolerable Risk to the System Hazards should be included). It is expected that the member states come up with the Index 47 log of system hazards. Secondly the Causal Analysis has to be carried out and linked to the 'System Hazards' of chapter 5.2 to ensure as well, that additional System Hazards arising from system design will be discovered.

After finishing these 'next steps' this chapter will contain the harmonised mandatory CCS safety requirements.

6.2 DB example for quantitative safety requirements

6.2.1 Preconditions

The considered hazards correspond to the Index 47 log of system hazards. Due to their close affinity, hazards no. 5&6, 9&10, 11&12, 13&14 and 19&20 are not considered separately. Because the operational condition of the test –track requires not all ETCS function defined in the CCS TSI annex A, the quantitative Safety Requirements presented here are restricted to that functionality and for this reason the TIRF distributed among its System Hazards is reduced to 70%. In general, two different fatalities (one at 40km/h, one at 200km/h) were applied to derive THRs from the TIRF resulting in two different THRs per hazard. (The intention was to meet the safety target also in degraded modes. In degraded modes the effect of a lower supervised max speed was taken into account by a lower fatality.)

6.2.2 Results of the Risk Analysis

The TIRF and the fatalities used in the risk analysis were defined on the basis of assessed statistic investigations. Based on the TIRF, assuming a criticality of 1 and the above mentioned fatality, the THRs for the different hazards were calculated (see chapter 6.2.3).

The TIRF (chapter 6.2.3) and the THR´s shown in chapter 6.2.4 is the basis for the safety case.

6.2.3 Relation of TIRF to THRs

TIRFETCS = 0,23 · 10-9 O/(R·h)

70% of the TIRFETCS is used for the restricted functionality of the pilot line. 10% of the tolerable risk is used to derive the quantitative safety requirements (only for random failures including handling errors).

$$TIRF_{ETCSpilotLine,randomFailures} = 0{,}1 \cdot 0{,}7 \cdot TIRF_{ETCS} = 1{,}61 \cdot 10^{-11} \frac{victims}{passenger \cdot hour}$$

This is in a first approach equally distributed among the pilot line's 13 ETCS System Hazards:

$$TIRF_{ETCSpilotLine,randomFailures,perHazard} = \frac{0{,}1 \cdot 0{,}7 \cdot TIRF_{ETCS}}{13}$$

$$TIRF_{ETCSpilotLine,randomFailures,perHazard} = 1{,}24 \cdot 10^{-12} \frac{victims}{passenger \cdot hour}$$

$$THR_{SystemHazard} = \frac{TIRF_{ETCSpilotLine,randomFailures,perHazard}}{F_k \cdot C_k}$$

Assuming a general criticality C=1:

$$THR_{SystemHazard} = \frac{TIRF_{ETCSpilotLine,randomFailures,perHazard}}{F_k}$$

As F, the fatality of the most fatal accident which may occur as consequence of a hazard is taken into consideration.

6.2.4 DB example of THRs

1	2	3	4	5	6
No	System hazard	average fatality at v=40km/h [victims / (passenger x accident)]	average fatality at v=200km/h [victims / (passenger x accident)]	THR (hazards/hour)	
				v=40km/h	v=200km/h
1	unauthorised setting back	$4 \cdot 10^{-4}$	$1 \cdot 10^{-2}$	$3{,}1 \cdot 10^{-9}$	$1{,}24 \cdot 10^{-10}$
2	passing the defined border of the shunting area (balise 'stop if in shunting')				
3	move inadmissibly authorised	$4 \cdot 10^{-4}$	$1 \cdot 10^{-2}$	$3{,}1 \cdot 10^{-9}$	$1{,}24 \cdot 10^{-10}$
4	permission to proceed not withdrawn in time in the event of danger	$4 \cdot 10^{-4}$	$1 \cdot 10^{-2}$	$3{,}1 \cdot 10^{-9}$	$1{,}24 \cdot 10^{-10}$
5	permissible speed as a function of route characteristics incorrectly shown	$4 \cdot 10^{-4}$	$1 \cdot 10^{-2}$	$3{,}1 \cdot 10^{-9}$	$1{,}24 \cdot 10^{-10}$
6	permissible speed as a function of route characteristics not enforced				
7	permissible speed when passing level crossings incorrectly shown				
8	permissible speed when passing level crossings not enforced				
9	permissible speed on account of the design of the overhead line incorrectly shown	$2{,}6 \cdot 10^{-5}$	$6{,}4 \cdot 10^{-4}$	$5 \cdot 10^{-8}$	$1{,}93 \cdot 10^{-9}$
10	permissible speed on account of the design of the overhead line not enforced				
11	permissible speed of train due to running properties of vehicles incorrectly shown	$4 \cdot 10^{-4}$	$1 \cdot 10^{-2}$	$3{,}1 \cdot 10^{-9}$	$1{,}24 \cdot 10^{-10}$
12	permissible speed of train due to running properties of vehicles not enforced				
13	permissible speed when running on sight incorrectly shown	$8{,}3 \cdot 10^{-4}$	--	$1{,}5 \cdot 10^{-9}$	-
14	permissible speed when running on sight not enforced				
15	permissible shunting speed incorrectly shown				
16	permissible shunting speed not enforced				

17	permissible speed when reversing incorrectly shown				
18	permissible speed when reversing in the event of danger not enforced				
19	permissible speed on grounds of track works incorrectly shown	0,77	0,77	$1{,}61 \cdot 10^{-12}$	$1{,}61 \cdot 10^{-12}$
20	permissible speed on grounds of track works not enforced				
21	lowering pantograph indication incorrectly shown	$2{,}6 \cdot 10^{-5}$	$6{,}4 \cdot 10^{-4}$	$5 \cdot 10^{-8}$	$1{,}93 \cdot 10^{-9}$
22	stopping at points where stopping is not permitted				
23	Information about route unsuitability not advised to the driver				
24	enter a section of the route which is not permitted to (due to route suitability)				
25	authorisation for reversing in the event of danger not given				
26	not stopping at the end of a movement authoritiy (without stopping beyond the end of movement authority)	$4 \cdot 10^{-4}$	$1 \cdot 10^{-2}$	$3{,}1 \cdot 10^{-9}$	$1{,}24 \cdot 10^{-10}$
27	not stopping at the end of a movement authoritiy (but stopping beyond the end of movement authority)	$4 \cdot 10^{-4}$	$1 \cdot 10^{-2}$	$3{,}1 \cdot 10^{-9}$	$1{,}24 \cdot 10^{-10}$
28	start moving without having a correct movement authority	$4 \cdot 10^{-4}$	$1 \cdot 10^{-2}$	$3{,}1 \cdot 10^{-9}$	$1{,}24 \cdot 10^{-10}$
29	air brake not applied when vehicle parked	$4 \cdot 10^{-4}$	$1 \cdot 10^{-2}$	$3{,}1 \cdot 10^{-9}$	$1{,}24 \cdot 10^{-10}$

6.2.5 Experience on working with the Risk Analyses (RA)

Even if the safety analysis is not finalised, it seems, that the safety target from the RA could be met at least for the condition of the ETCS pilot line of DB.

The defined hazards are on a high functional level, thus it can be assumed, that the risk analysis will be stable even if technical functionality or operational regulations will be adapted / modified in future.

The mapping of the safety requirements to the industrial product has required a deep co-operation between the railway and the supplier. In future the effort could be minimised by providing a description of the operational assumptions (incl. human factor) to the supplier.

One issue of a risk analysis is to derive a safety target in form of an acceptable risk (TIRF). The allocation to different hazards and the transformation to hazard rates is another important step in order to join the risk analysis and the hazard analysis of the supplier. The

TIRF is the fundamental value which has to be fulfilled, whereas the distribution of the TIRF to the THRs may alter due to the applied system design and the appropriate Causal Analysis. The experience during the process of adapting the suppliers' Causal Analysis to the risk analysis showed that the safety requirements can be reduced by a factor up to 10 taking into account:

- That the hazards from the RA do not reflect, that only a few causes have a major influence on several hazards (they should not be considered repeatedly).
- The analysis of the causes on the basis of the railway specific operational conditions can reduce the requirements in addition as well as
- the analysis of the criticality for different hazards.

As expected the influence of the operational handling is the most important one. Further investigation has to consider processes of the train data entry (especially the max. speed of the train and the train length) and the entry of temporary speed restrictions on track-side.

6.3 UK example for quantitative safety requirements

No.	Ref.	System hazard	UK Safety Req	UK Rationale
1	[4.7.2-2]	unauthorised setting back	**10^{-9}/hr**	Amend wording to 'Unauthorised movement in reverse direction'.
2	[4.8.2]	passing the defined border of the shunting area (balise 'stop if in shunting')	**10-5/hr**	Same Rationale as 23, 24, 25. Ensure that shunting is not authorised without a Balise List being issued without operational controls being in place. A 'shunting overlap' is required to protect against propelling moves and/or the stopping distance after the emergency brake has been triggered. Reliant on reading a single balise/balise group. Operational rules and layout of the track currently provide the main protection and this situation is assumed to continue and thus a low safety requirement is used.
3	[5.1-2]	move inadmissibly authorised	**10-9/hr**	Core functionality of train control system. Maximum level of safety realistically attainable. Taken to include safety of trackworkers in a protected area.
4	[5.1-3]	permission to proceed not withdrawn in time in the event of danger	**10-4/hr**	Delete 'in time in the event of danger'. Due to quality of service, it is important that the UK does not rely on ETCS alone for removal of movement authorities and continues to use voice communication as well. Within this hazard the reliability of the datalink is included. Control of hazard is dominated by the ability to discover the hazardous circumstances in practice. There would be very significant GSM-R cost implications should this requirement be made more demanding.

5	[6.1-0]	Permissible speed as a function of route characteristics not shown to the driver	**10-4/hr**	UK philosophy is that safety is in the enforcement system rather than the driver/displayed information and hence the display system is only marginally safety related. Hazard associated by enforcement is covered in the next hazard. Considered only as permanent static speed profile. Temporary and emergency speed restrictions considered at 30xxx.
6	[6.1-1]	Permissible speed as a function of route characteristics not enforced	**10-7/hr speeds up to & including 25% overspeed;** **10-9/hr speeds in excess of 25% overspeed;**	UK philosophy is that safety is in the enforcement system rather than the driver/displayed information and hence the enforcement system provides the safety. It is considered that there is an element of mitigation in the driver not speeding excessively due to his route knowledge. Assumes that there are sufficient definitions of train types to cater for hazards such as train/OHLE compatibility.
7	[6.1.1.3-0]	max. permissible speed when passing level crossings is not shown to the driver	**10-4/hr**	UK philosophy is that safety is in the enforcement system rather than the driver/displayed information and hence the display system is only marginally safety related. Hazard associated by enforcement is covered in the next hazard.

8	[6.1.1.3-1]	max. permissible speed when passing level crossings is not enforced	**10-7/hr speeds up to & including 25% overspeed;** **10-9/hr speeds in excess of 25% overspeed;**	UK philosophy is that safety is in the enforcement system rather than the driver/displayed information and hence the enforcement system provides the safety. It is considered that there is an element of mitigation in the driver not speeding excessively due to his route knowledge. Consequences for level crossing may be different but not considered to be a material affect based on preliminary assessment.
9	[6.1.1.8-0]	max. permissible speed on account of the design of the overhead line is not shown to the driver	**NA**	Not required by UK, fully covered by items 5 & 6.
10	[6.1.1.8-1]	max. permissible speed on account of the design of the overhead line is not enforced	**NA**	Not required by UK, fully covered by items 5 & 6.
11	[6.1.2.1-0]	max. permissible speed of train due to running properties of vehicles is not shown to the driver	**10-4/hr**	UK philosophy is that safety is in the enforcement system rather than the driver/displayed information and hence the display system is only marginally safety related. Hazard associated by enforcement is covered in the next hazard.

12	[6.1.2.1-1]	max. permissible speed of train due to running properties of vehicles is not enforced	**10-7/hr speeds up to & including 10% overspeed;** **10-9/hr speeds in excess of 10% overspeed;**	UK philosophy is that safety is in the enforcement system rather than the driver/displayed information and hence the enforcement system provides the safety. It is considered that there is an element of mitigation in the driver not speeding excessively due to his route knowledge. Note: Relies on data entry.
13	[6.1.3.1-0]	max. permissible speed when running on sight is not shown to the driver	**NA**	Given that this speed is only optionally displayed, it cannot have a safety requirement.
14	[6.1.3.1-1]	max. permissible speed when running on sight is not enforced	**10-7/hr speeds up to & including 25% overspeed;** **10-9/hr speeds in excess of 25% overspeed;**	UK philosophy is that safety is in the enforcement system rather than the driver/displayed information and hence the enforcement system provides the safety. It is considered that there is an element of mitigation in the driver not speeding excessively due to his route knowledge.
15	[6.1.3.2-0]	permissible shunting speed is not shown to the driver	**NA**	Given that this speed is only optionally displayed, it cannot have a safety requirement.
16	[6.1.3.2-1]	permissible shunting speed is not enforced	**10-4/hr**	To be controlled by operational process in the UK. Low value required. Risks considered generally to be mitigated by low speed of operation. Speed enforcement functions are likely to be dominated by the most demanding speed enforcement requirement.
17	[6.1.3.4-0]	permissible speed when reversing is not shown to the driver	**NA**	Given that this speed is only optionally displayed, it cannot have a safety requirement.
18	[6.1.3.4-1]	permissible speed when reversing in the event of danger not enforced	**NA**	To be controlled by operational process in the UK. Not intending to use this functionality in the UK.

19	[6.1.3.7-0]	max. permissible speed on grounds of track works is not shown to the driver	**NA**	Hazard relates to protection of trackworkers only.
20	[6.1.3.7-1]	max. permissible speed on grounds of track works is not enforced	**10-7/hr**	Hazard relates to protection of trackworkers only. Scenarios considered – reducing linespeed on the line where the workers are working to enable red zone arrangements to be established and reducing linespeed on open lines adjacent to workers.
21	[6.2.1-0]	lowering pantograph information is not shown to driver	**NA**	Controlled by Operational process in UK.
22	[6.2.8]	stopping at points where stopping is not permitted	**10-4/hr**	Primarily controlled by operational process in UK.
23	[6.2.10-0]	Information about unsuitability not advised to the driver	**10-4/hr**	In the UK this hazard is adequately controlled through existing operational procedures. The UK will reinforce this operational control of this hazard even when ETCS is implemented. Therefore a SIL0 target has been assigned.
24	[6.2.10-1]	enter a section of the route which is not permitted to	**10-4/hr**	In the UK this hazard is adequately controlled through existing operational procedures. The UK will reinforce this operational control of this hazard even when ETCS is implemented. Therefore a SIL0 target has been assigned.
25	[6.2.11]	Authorisation for reversing in the event of danger not given		
26	[6.4.1-1]	signal passed at danger (without train stopping afterwards)	**10-9/hr**	Change ’Signal’ to ‘Danger Point’ Highest integrity realistically achieved. Workshop assumption is that this relates to errors in definition to where the train should stop. No braking - Justification Report to be clarified.

27	[6.4.1-2]	not stopping at a signal at danger in time	**10-9/hr**	Change 'Signal' to 'Danger Point' Highest integrity realistically achieved. Since the System Definition includes the Driver entering the data, this value is only achievable if the system protects against data entry errors. Insufficient braking – Justification Report to be clarified.
28	[6.4.1-3]	starting move towards a signal at danger	**10-9/hr**	Add 'and proceeding past Danger Point'. Highest integrity realistically achieved. Since the System Definition includes the Driver entering the data, this value is only achievable if the system protects against data entry errors. Justification Report to be clarified.
29	[7.2.1]	air brake not applied when vehicle stabled	**10-4/hr**	Replace description with 'Brake not commanded when vehicle parked'. Low value since safety resides elsewhere ie in the braking system.
30	new	Voice radio unavailable to warn Driver of dangerous situation	**EIRENE availability value**	Add Safety requirement based on EIRENE availability – principally to drive similar availability requirements into supporting infrastructure eg power supplies and application of EIRENE to trains and infrastructure.
31	new	Train detection failure due to EMC Train to Trackside & Static Parameters not complied with	**10-7/hr**	Probability of not complying with the static parameters and Gabarit in Annex A Appendix 1 thus causing the train detection to fail wrongside. See attachment providing justification.
32	new	Giving authority to the rear train where two trains are within section	**10-9/hr**	Where train is on same train detection, eg a split train, and the rear train is given the movement authority. Could arise through a variety of circumstances eg train splitting, train assisting faulty train and train SPADing into section. May require more than one THR for different circumstances.

33		Temporary speed restriction not enforced	**10-7/hr speeds up to & including 10% overspeed;** **10-9/hr speeds in excess of 10% overspeed;**	Application/Data preparation likely to be the key issue. The safety feature will therefore be driven by the procedures. Includes emergency speed restrictions. Need to consider further the tolerance rating stated with Civil/Wagon Engineer.

7 Reference

Ref #	Document
1	Justification Report for Safety Requirements and Requirements to Safety Analysis for Interoperability for the Control-Command and Signalling Sub-System.
2	Directive 96/48/EC of 23 July 1996 on the interoperability of the trans-European high-speed rail system
3	Directive 2001/16/EC of 19 March 2001 on the interoperability of the trans-European conventional rail system
4	Commission Decision of 30 May 2002 concerning the technical specification for interoperability relating to the control-command and signalling subsystem of the trans-European high-speed rail system referred to in Article 6(1) of Council Directive 96/48/EC (notified under document number C(2002) 1947)
5	CCS TSI CR: 2001/16/EC - 01/16-ST01 part 2 Version EN 07 24.11.2004
6	Index 27/UNISIG Subset 91 Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2
7	All Class 1 specifications for ETCS as defined in Annex A of the Control-Command and Signalling Technical Specification for Interoperability
8	Functional Analysis Of Trans – European Rail Operation Reference EEIG:01 E 129 version 2 dated 08.07.04